



11-07-02

2132  
#4  
SP  
12-503

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:

WHEELER et al. )

Serial No.: 09/923,075 )

Filed: August 6, 2001 )

For: *Modifying Message Data and  
Generating Random Number Digital* )

*Signature Within Computer Chip* )

Docket No.: 10399-34383 )

Art Unit:

Examiner:

Charlotte, North Carolina

Commissioner for Patents  
Washington, D.C. 20231

RECEIVED

NOV 08 2002

Technology Center 2100

INFORMATION DISCLOSURE STATEMENT

In compliance with the Applicant's duty of disclosure under 37 CFR §1.56, Applicant brings the attached document or documents cited on the attached form PTO/SB/08 to the attention of the U.S. Patent and Trademark Office in accordance with the provisions of 37 CFR §1.97-98.

Nothing herein—including the submission of the documents themselves, whether in this or any other filing—constitutes an admission by Applicant that any of the documents is prior art with respect to the present invention, or a waiver of any rights of Applicant. Indeed, while each citation includes a date, it should be understood that, whether expressly stated or not, the date specified in the citation is a date as alleged by the document or otherwise, and Applicant neither admits nor denies the correctness of the specified date at this time. Moreover, with regard to non-patent documents, Applicant neither admits nor denies that each document submitted is, in fact, a "publication" within the meaning of 35 U.S.C. §102.

Respectfully submitted,

*Chad D. Tillman*

Chad D. Tillman

U.S. Reg. No. 38,634

MORRIS, MANNING & MARTIN, L.L.P.

6000 Fairview Road, Suite 1125

Charlotte, NC 28210

Telephone (704) 554-7070; Fax (704) 556-9554



Please type a plus sign (+) inside this box → ☐

PTO/SB/08B (10-96)  
Approved for use through 10/31/99. OMB 0651-0031  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.



Substitute for form 1449B/PTO		<b>Complete if Known</b>			
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (use as many sheets as necessary)		Application Number	09/923,075		
		Filing Date	08/06/2001		
		First Named Inventor	Wheeler et al.		
		Group Art Unit			
		Examiner Name			
Sheet	1	of	5	Attorney Docket Number	10399-34383

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
	1.	BURTON S. KALISKI, JR., Some Examples of the PKCS Standards, An RSA Laboratories Technical Note, 11-1-93, RSA Laboratories, Redwood City, CA, pp. 1-15	
	2.	BURTON S. KALISKI, JR., A Layman's Guide to a Subset of ASN.1, BER, and DER, An RSA Laboratories Technical Note, 11-1-93, RSA Laboratories, Redwood City, CA, pp. 1-37	
	3.	PKCS Editor, PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, Draft 2, 1-5-2001, RSA Laboratories, Bedford, MA, pp. 1-60	
	4.	PKCS #3: Diffie-Hellman Key-Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, 11-1-93, RSA Laboratories, Redwood City, CA, pp. 1-8	
	5.	PKCS #6: Extended-Certificate Syntax Standard, An RSA Laboratories Technical Note, 11-1-93, Version 1.5, RSA Laboratories, Redwood City, CA, pp. 1-11	
	6.	PKCS #8: Private-Key Information Syntax Standard, An RSA Laboratories Technical Note, 11-1-93, Version 1.2, RSA Laboratories, Redwood City, CA, pp. 1-5	
	7.	MICHAEL J. WIENER, Performance Comparison of Public-Key Cryptosystems, The Technical Newsletter of RSA Laboratories, a division of RSA Data Security, Inc., Summer 1998, Vol. 4, Number 1, RSA Laboratories, San Mateo, CA, pp. 1-23	
	8.	GEORGE APOSTOLOPOULOS, et al., Securing Electronic Commerce: Reducing the SSL Overhead, IEEE Network, July/Aug. 2000, Vol. 14, Issue 4, pp. 1-16	
	9.	UELI MAURER, Modelling a Public-Key Infrastructure, Sept. 1996, Proc. 1996 European Symposium on Research in Computer Security, Lecture Notes in Computer Science, Berlin: Springer-Verlag, Rome, Italy, Department of Computer Science, Swiss Federal Institute of Technology, Zürich, Switzerland, pp. 1-26	
	10.	Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1, 1-11-94, pp. 1-45, CSL Bulletin For FIPS 140-1 pp. 1-6, Validated FIPS 140-1 Cryptographic Modules 2001, 2000, 1999, 1998, 1997-95, pp. 1-14	
	11.	MARK HEROUX, A Private Key Storage Server for DCE -- Functional Specification, Open Software Foundation Request for Comments: 94.1, November 1996, (web site at <a href="http://www.opengroup.org/rfc/mirror-rfc/rfc94.1.txt">http://www.opengroup.org/rfc/mirror-rfc/rfc94.1.txt</a> ), date of capture 6/13/01, pp. 1-73	

RECEIVED  
NOV 08 2002  
Technology Center 2100

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.





Please type a plus sign (+) inside this box → ☐

PTO/SB/08B (10-96)  
Approved for use through 10/31/99. OMB 0651-0031  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

+

<b>Substitute for form 1449B/PTO</b>  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  <i>(use as many sheets as necessary)</i>			<b>Complete if Known</b>		
			<b>Application Number</b>	09/923,075	
<b>Sheet</b>	2	<b>of</b>	5	<b>Filing Date</b>	08/06/2001
			<b>First Named Inventor</b>	Wheeler et al.	
			<b>Group Art Unit</b>		
			<b>Examiner Name</b>		
			<b>Attorney Docket Number</b>	10399-34383	

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS		
Examiner Initials <sup>*</sup>	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	12.	PETER COX, Bench-Marking SmartGate, Establishing the Scalability of V-ONE's SmartGate Security System, Internet SmartWare Ltd., 7-24-97, pp. 1-7
	13.	Answers to Frequently Asked Questions about Today's Cryptography, RSA Data Security, Inc., 10-5-1993, Revision 2.0, pp. 1-44
	14.	Announcing the Standard for Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186, 5-19-94, pp. 1-18
	15.	SHARON BOEYEN, Certificate Policies and Certification Practice Statements, Entrust Technologies White Paper, February 1997, Version 1.0, pp. 1-7
	16.	Public-Key Infrastructure (PKI) - The VeriSign Difference, 2-3-2001, Copyright 1999, VeriSign, Inc., pp. 1-21
	17.	THIERRY MOREAU, Thirteen Reasons to Say 'No' to Public Key Cryptography, Draft paper, 3-4-98, CONNOTECH Experts-Conseils, Inc., Montréal, Québec, Canada, pp. 1-5
	18.	"X9 Overview," American Bankers Association web page (web site at <a href="http://www.x9.org/aboutX9.htm">http://www.x9.org/aboutX9.htm</a> ), 1998, date of capture 1/11/99, 3 pp.
	19.	July 1997 Meeting Report, Electronic Payments Forum (web site at <a href="http://www.epf.net/PrevMtngs/July97Mtng/July97Report.htm">http://www.epf.net/PrevMtngs/July97Mtng/July97Report.htm</a> ), date of capture 1/11/99, 2 pp.
	20.	Hettinga's Best of the Month, Journal of Internet Banking and Commerce, 1-5-98, (web site at <a href="http://www.arraydev.com/commerce/JIBC/9801-20.htm">http://www.arraydev.com/commerce/JIBC/9801-20.htm</a> ), date of capture 1/11/99, 6 pp.
	21.	BURTON S. KALISKI JR., An Overview of the PKCS Standards, An RSA Laboratories Technical Note, 11-1-93, RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS), pp. 1-27
	22.	Public Key Cryptography, NIST Special Publication 800-2, April 1991, reprinted at <a href="http://csrc.nist.gov/publications/nistpubs/800-2/800-2.txt">http://csrc.nist.gov/publications/nistpubs/800-2/800-2.txt</a> , pp. 1-138

RECEIVED  
NOV 08 2002  
Technology Center 2100

<b>Examiner Signature</b>		<b>Date Considered</b>	
---------------------------	--	------------------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

+



Please type a plus sign (+) inside this box → +

PTO/SB/08B (10-96)  
Approved for use through 10/31/99. OMB 0651-0031  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

+

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  <i>(use as many sheets as necessary)</i>			<b>Complete if Known</b>		
			Application Number	09/923,075	
			Filing Date	08/06/2001	
			First Named Inventor	Wheeler et al.	
			Group Art Unit		
			Examiner Name		
Sheet	3	of	5	Attorney Docket Number	10399-34383

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS		
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	23.	Guideline for Implementing Cryptography in the Federal Government, NIST Special Publication 800-21, November 1999, pp. 1-138
	24.	Guideline for the Use of Advanced Authentication Technology Alternatives, FIPS Publication 190, September 28, 1994, reprinted at <a href="http://csrc.nist.gov/publications/fips/fips190/fip190.txt">http://csrc.nist.gov/publications/fips/fips190/fip190.txt</a> , pp. 1-55
	25.	Building A Foundation of Trust in the PC, The Trusted Computing Platform Alliance, January 2000 (web site at <a href="http://www.trustedpc.org">http://www.trustedpc.org</a> ), pp 1-9
	26.	Trusted Platform Module (TPM) Security Policy (A Part of the "TCPA Security Policy"), Version 0.45, October 2, 2000, pp. 1-13
	27.	Trusted Platform Module Protection Profile (TPMPP) (A Part of the "TCPA Security Policy"), Version 0.45, September 14, 2000, pp. 1-151
	28.	TCPA PC Specific Implementation Specification, Version 0.95, July 4, 2001, pp. 1-70
	29.	Common Criteria for Information Technology Security Evaluation, Smart Card Security User Group, Smart Card Protection Profile, draft Version 2.1d, March 21, 2001, pp. 1-194
	30.	X9.84-2000, Biometric Information Management and Security for the Financial Services Industry, draft version, December 2000, pp. 1-141
	31.	Security Requirements for Cryptographic Modules, FIPS Publication 140-2, May 25, 2001, pp. 1-62
	32.	Secure Hash Standard, FIPS Publication 180-1, April 17, 1995, pp. 1-24
	33.	Digital Signature Standard (DSS), FIPS Publication 186-2, January 27, 2000, pp. 1-72

**RECEIVED**  
NOV 08 2002  
Technology Center 2100

Examiner Signature	Date Considered
--------------------	-----------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

+



Please type a plus sign (+) inside this box → ☐

PTO/SB/08B (10-96)  
Approved for use through 10/31/99. OMB 0651-0031  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (use as many sheets as necessary)			<b>Complete if Known</b>		
			Application Number	09/923,075	
			Filing Date	08/06/2001	
			First Named Inventor	Wheeler et al.	
			Group Art Unit		
			Examiner Name		
Sheet	4	of	5	Attorney Docket Number	10399-34383

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
	34.	Entity Authentication Using Public Key Cryptography, FIPS Publication 196, February 18, 1997, pp. 1-52	
	35.	Computer Data Authentication, FIPS Publication 113, May 30, 1985, (web site at <a href="http://www.itl.nist.gov/fipspubs/fip113.htm">www.itl.nist.gov/fipspubs/fip113.htm</a> ), date of capture 1/16/01, pp. 1-7	
	36.	Hettinga's Best of the Month, Journal of Internet Banking and Commerce, March 31, 1999, (web site at <a href="http://www.arraydev.com/commerce/JIBC/9801-20.htm">http://www.arraydev.com/commerce/JIBC/9801-20.htm</a> ), pp. 1-4	
	37.	The Electronic Commerce Challenge, Journal of Internet Banking and Commerce, March 31, 1999, (web site at <a href="http://www.arraydev.com/commerce/JIBC/9811-06.htm">http://www.arraydev.com/commerce/JIBC/9811-06.htm</a> ), pp. 1-2	
	38.	Sales Brochure for APPROVEIT, electronic approval management software, by SilanisTechnology, Inc., July 18, 2000, pp. 1-12	
	39.	Public Key Infrastructure, An NSS Group White Paper, by Bob Walder, undated, reprinted from website <a href="http://www.nss.co.uk/WhitePapers/PublicKeyInfrastructure.htm">http://www.nss.co.uk/WhitePapers/PublicKeyInfrastructure.htm</a> on January 25, 2001, pp. 1-18	
	40.	Smart Card & Security Basics, Cardlogix, Inc. brochure, Ref. date: Q1-Q2 2000, pp. 3-36	
	41.	Understanding Public Key Infrastructure (PKI), Technology White Paper, by RSA Security, Inc., 1999, pp. 1-10	
	42.	An Overview of Smart Card Security, Chan, Siu-cheung Charles, August 17, 1997, reprinted from website <a href="http://home.hkstar.com/~alanchan/papers/smartCardSecurity/">http://home.hkstar.com/~alanchan/papers/smartCardSecurity/</a> on January 27, 2001, pp. 1-7	
	43.	Technical Introduction to CIP 3.0, Taschler, Scott, September 30, 1997, reprinted from website <a href="http://www.datakey.com/cardpage/cip.htm">http://www.datakey.com/cardpage/cip.htm</a> on January 25, 2001, pp. 1-6	
	44.	Smart Cards: Enabling Smart Commerce in the Digital Age, CREC/KPMG White Paper (Draft), May 1998, pp. 1-22	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Substitute for form 1449B/PTO

## INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	5	of	5
-------	---	----	---

**Complete if Known**

Application Number	09/923,075
--------------------	------------

<b>Filing Date</b>	08/06/2001
--------------------	------------

<b>First Named Inventor</b>	<b>Wheeler et al.</b>
-----------------------------	-----------------------

### Group Art Unit

Examiner Name

Attorney Docket Number	10399-34383
------------------------	-------------

## OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

[illegible]

Examiner  
Signature

Date  
Considered

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number. <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

**Burden Hour Statement:** This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO:** Assistant Commissioner for Patents, Washington, DC 20231.